

Remarks

Claims 1-33 are pending. By this Amendment, claims 1, 6, 12-15, 17-21, 24 and 30-32 are amended. Reconsideration in view of the above amendments and following remarks is respectfully requested.

Applicant appreciates the courtesies extended by Examiner to Applicant and Applicant's representative during the October 6 telephonic interview. The points discussed during the telephonic interview are incorporated herein.

I. The Claims Define Patentable Subject Matter Pursuant to 35 USC 103

The Office Action rejects claims 1-33 under 35 U.S.C. as being anticipated by U.S. Patent No. 6,519,703 to Joyce (hereinafter "Joyce"). The rejection is respectfully traversed.

The Office Action asserts that Joyce discloses a method for detecting unauthorized intrusion in a network system, including the steps of receiving packet level activity information from the network, sorting port specific activity information from the received packet level activity information by IP/user, converting the sorted IP/user port specific activity information to human behavioral measures of intent, monitoring the converted human behavioral measures and executing at least one of a blocking action based upon the monitored human behavior measures.

Joyce is directed to a method for analyzing individual packets on a packet by packet basis in a computer network using a heuristic firewall. In Joyce, each individual packet is monitored by port as opposed to an IP/User. Each packet is judged on an individual basis and packets that are discarded if they are deemed to have 'poor confidence'. Thus, the system of Joyce is not

capable of detecting and monitoring various intrusion patterns that occur across time and that are comprised of multiple and complex combinations of packets or detecting new and previously undetected behaviors by separate IP/users.

The Office Action asserts that Joyce discloses the step of “sorting port specific activity information from the received packet level activity information by IP/user (see col. 4, lines 13-16).” However, at col. 4, Joyce is only disclosing the pulling of port and time-stamped information from raw data packets to feed a corresponding heuristic stage. This does not equate to or even suggest collecting sequential samples of sorted port and NON-port specific activity/behavior from the received packet level activity for each IP/user. This aspect of the invention allows assessment of each user as opposed to unattributed packets, in contrast to Joyce.

The Office Action further asserts that Joyce discloses “converting the sorted/IPuser port specific activity information to human behavioral measures (see col. 2, lines 41-65, col. 3, lines 29-58) monitoring the converted human behavioral measures (see col. 2 lines 41-65, col. 3, lines 29-58, col. Lines 13-16, 50-54).” However, Joyce only discloses classifying each packet as having “high confidence,” “marginal confidence” or “poor confidence.” Classifying each packet in this manner only involves determining whether an individual packet matches a predetermined criteria for ‘confidence.’ This type of classification of packets does not teach converting packet level activity into human behaviors and activities for each IP/user and converting the sorted IP/user behavioral activities into behavioral measures of expertise and deception as measures of underlying intent for IP/user, as recited in claim 1. It also does not teach monitoring sequential determinations of the converted human intent behavioral measures for the duration that each

IP/user is in the network, wherein the monitoring step includes determining new and previously undetected misuse behaviors as indicated by increased intent levels of expertise and deception, as recited in claim 1. Thus, the invention provides for an assessment of each IP/user by characterizing each user rather than assigning a predetermined criteria to a specific packet.

The Office Action also asserts that Joyce discloses “executing at least one blocking action based upon the monitored human behavioral measures (see col. 2, lines 51-54, col. 3, lines 1-16, 43-58). However, Joyce merely describes a packet analysis whereby if packets are deemed ‘marginal confidence’ they are released into a more complex firewall rule base for processing and if they are deemed ‘poor-confidence’ they are shunted out of the firewall. Joyce does not however teach executing at least one network connection blocking action or passive gathering of tracked intent information for any given IP/user if monitored expertise and deception measures exceed intent thresholds underlying non-misuse network activity, as recited in claim 1. Thus, the claimed invention examines overall behavior, and defines normal measures of expertise and deception contained in multiple and complex collections of activities/behaviors comprised of numerous packets and then detects and identifies deviations from the normal based on thresholds established for human intent..

Thus, in Applicant’s invention, the system converts the network activity to a behavior assessment based upon determinations of expertise (E) and deception (D). The invention then tracks these behavior assessments and blocks certain activity based upon these behavior assessments without regard to the specific packets. In addition, the invention is not a firewall as described in Joyce.

Therefore, Joyce fails to teach the features of claim 1. Similarly, Joyce fails to disclose a system for preventing unauthorized intrusion in a network system that includes a traffic sorter that receives *a copy* of the network activity and sorts such activity by IP/users; and an activity monitor operatively coupled to the traffic sorter for monitoring converted human behavior measures by IP/users, that is based upon a copy of the network activity, as recited in claim 12. Further, Joyce fails to disclose an inter-port fusion module that fuses assessments from one or more assessment engines that monitor behavior measures – not packets - , as recited in claim 12.

Thus, Joyce fails to disclose the features recited in independent claims 1 and 12. It is respectfully submitted that independent claims 30 and 31 are also distinguishable over the applied reference for reasons similar to those described in connection with claim 1 above. Further, dependant claims 2-11 and 13-29 are likewise distinguishable for at least the reasons described above. Therefore, withdrawal of the rejection of claims 1-31 under 35 U.S.C. § 103 is respectfully requested.

CONCLUSION

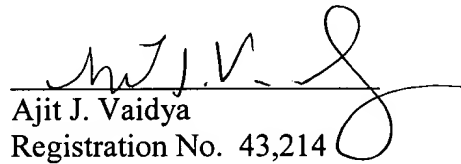
In view of the foregoing, applicant respectfully requests reconsideration and the allowance of the above-identified application. Should the Examiner feel that there are any issues outstanding after consideration of this response, the Examiner is invited to contact Applicant's representative at the telephone number listed below.

If there are any other fees due in connection with the filing of this response, please charge the fees to our Deposit Account No. 50-1349. If a fee is required for an extension of time under 37 C.F.R. § 1.136 not accounted for above, such an extension is requested and the fee should also be charged to our Deposit Account.

Respectfully submitted,

Dated: November 15, 2005

HOGAN & HARTSON LLP
555 13th Street, N.W.
Washington, D.C. 20004
(202) 637-5600
Customer No.: 24633


Ajit J. Vaidya
Registration No. 43,214